



THE CORPORATE COUNSEL'S GUIDE TO OPEN SOURCE SOFTWARE POLICY IMPLEMENTATION



GUIDE BOOK

General counsels increasingly face a dilemma – how to enable enterprise software development teams to efficiently leverage open source software (OSS) while guarding against licensing risks. OSS is software for which the source code is made available under a copyright license. Software development teams can use, change and improve the software and can redistribute it in modified or unmodified form. It is often developed in a public, collaborative manner, and it is easily available online.

Companies must reduce budgets while continuing to deliver innovative software applications that differentiate them in an increasingly competitive marketplace. This is why so many companies rely on OSS to complete software projects with fewer coding resources.

Lawyers can help the enterprise benefit from OSS adoption by establishing guidelines for OSS use that protect the enterprise while enabling development teams to meet their business objectives. The legal staff must protect the enterprise against risk without creating policies that impede business agility.

Successfully implementing OSS raises questions that internal legal counsel must be able to answer, such as:

- How can I avoid OSS license infringement lawsuits?
- How can I help development teams ensure licensing compliance – without creating a drain on our legal team and our budget for outside counsel?
- How can I be sure that the software we're developing does not include software components that violate licensing?
- How do we conduct due diligence for potential acquisitions to ensure the validity of software code that our company might acquire?
- How can we gather the information that lawyers, software developers and export personnel need to ensure compliance?

- How can I help our software development team take advantage of the economic efficiencies of OSS without slowing down development?

MITIGATING THE RISKS OF OPEN SOURCE SOFTWARE

A company's ability to effectively find, integrate, and manage OSS is as important as its own internal development capabilities.

The key to avoiding the consequences of improperly using open source code is to develop policies and procedures based on best practices and automating the management of OSS code. Legal counsel should understand the obligations associated with OSS licenses, and must foster the development of cross-departmental policies for avoiding the business risks of violating software licenses.

“Free code” does not mean “free of obligations.” Open source brings unique and sometimes complex license and business risks that can delay, and potentially prevent, software deployment or shipment if not properly managed. A U. S. Federal appeals court decision in the Jacobsen vs. Katzer case determined that Katzer had improperly used open source and was liable for copyright infringement as well as breach of contract. While this case set a new standard for open source license enforcement, it has also raised awareness of the importance of explicitly managing open source code.

Compliance with open source license obligations is key to avoiding the risk of costly and time-consuming litigation. Once a mere matter of proper attribution between developers and businesses, open source has now moved into the realm of the courts. In addition, the publicity surrounding open source licensing issues can threaten the reputation and relationships of the defendant. Improperly managed open source code can result in bad publicity, copyright infringement and even stop shipment orders

that can damage company reputations and immediately impact product revenue streams.

There are notable examples of companies having to respond to charges that they did not adequately manage their use of open source code. Diebold was subject to a GPL infringement lawsuit over using Linux in its voting machines without complying with the GNU public license, and Google received bad publicity during the launch of its Android mobile platform because of known security liabilities. Skype was sued for violating the GPL license for a VoIP phone, and Verizon was sued over the software license for OSS used in its wireless routers.

Manual methods of finding, selecting, monitoring and validating open source code are an unmanageable drain on law departments. Automation is essential so your company can efficiently incorporate OSS into its development efforts to drive down costs and efficiently manage applications throughout their lifecycles.

IMPLEMENTING BEST PRACTICES

Solutions from Black Duck allow software development executives to implement best practices while streamlining development and making most efficient use of development resources. The following are just a few of the best practices that you will be able to implement:

- Reuse existing components wherever appropriate
- Track and control changes to internal components
- Control reviews of sensitive or external components
- Verify every build and release
- Review compliance at project phase transition
- Create an audit trail of OSS usage
- Control component utilization
- Assess software components before making an acquisition

RELYING ON AUTOMATION TO IMPROVE PRODUCTIVITY

Black Duck is the leading global provider of tools for accelerating software development through the management of open source and third-party code. Black Duck enables companies to shorten time to market and reduce development and maintenance costs while mitigating the risks and challenges associated with open source reuse, including license obligations, security vulnerabilities, and version proliferation.

The ability to easily find and assess the best open source components is essential. The Black Duck® KnowledgeBase™ – which tracks greater than a million unique OSS projects – is the industry's most comprehensive database of OSS and associated licenses and other information.

The successful use of open source requires treating the management of OSS as an integrated, cross-departmental business process, not simply a development process. Automation technology can streamline processes necessary for successfully managing the proper integration of code from many sources, and it can allow your software development teams to analyze the risks according to policies driven by legal counsel.

Attorneys can also leverage solutions from Black Duck to comply with export laws, such as the U.S. laws governing the export of software containing encryption. Black Duck offers the world's first and only solution specifically designed to facilitate encryption export compliance management for software and for electronic devices containing software. Legal counsel worldwide depend on Black Duck solutions to analyze source code and identify cryptography within code to more quickly and easily comply with government licensing and documentation requirements for distributing software internationally.

The enterprise can now rely on automated systems that liberate lawyers from conducting cumbersome legal reviews for the use of open source code. You can integrate your legal team with security, software development and other policy-making authorities within your company to streamline the use of OSS according to defined policies and procedures.

RELYING ON BLACK DUCK

It is impractical for any enterprise development organization to track and update the enormous pool of available open source code and its associated metadata. The KnowledgeBase includes greater than a million unique projects from more than 8,400 sites and is updated with thousands of new products on a regular basis. Black Duck captures extensive metadata on open source code, and the KnowledgeBase is continuously expanded. Black Duck has helped hundreds of companies automate the use of OSS, and some of the largest software companies in the world have standardized on Black Duck solution for implementing corporate policies without disrupting development efforts.

Black Duck provides a framework that allows attorneys to access timely and relevant information about OSS components used by the enterprise to effectively manage business risks. By automating the use of open source, you can effectively manage licensing compliance according to enterprise policies and procedures. To find out how your company can automate OSS implementations according to best practices, visit www.blackducksoftware.com.

ABOUT BLACK DUCK SOFTWARE

Black Duck provides the world's only end-to-end [OSS Logistics](#) solution, enabling enterprises of every size to optimize the opportunities and solve the logistical challenges that come with open source adoption and management. As part of the greater open source community, Black Duck connects developers to comprehensive OSS resources through [The Black Duck Open Hub](#) (formerly Ohloh), and to the latest commentary from industry experts through the [Open Source Delivers](#) blog. Black Duck also hosts the [Open Source Think Tank](#), an international event where thought leaders collaborate on the future of open source. Black Duck is headquartered near Boston and has offices in San Mateo, London, Paris, Frankfurt, Hong Kong, Tokyo, Seoul, and Beijing. For more information about how to leverage open source to deliver faster innovation, greater creativity, and improved efficiency, visit www.blackducksoftware.com and follow the company at [@black_duck_sw](#).

CONTACT

To learn more, please contact: sales@blackducksoftware.com or 1.781.891.5100
Additional information is available at: www.blackducksoftware.com

JUSTIFYING M&A ACTIVITY

Voxeo Corporation makes voice applications easy to build and deploy and as it sought to grow its business through the acquisition of an innovative Asian developer, management performed a rapid assessment of the value of the target company's software code base. According to Voxeo Vice President of Engineering Daniel Polfer, "We recognize that intellectual property laws vary throughout the world, and we wanted to fairly evaluate the code of the company we were acquiring to protect our investment and understand and document the value of the code." Manually evaluating the code was impractical, so Voxeo turned to Black Duck. A cross-departmental team consisting of legal counsel and engineering executives analyzed the code – and then proceeded through the acquisition with confidence.

"Before writing the check for the acquisition, we needed to identify what open source the company used and how they had used it," said Polfer. "Before we completed the deal, we were able to reduce our business risk by objectively assessing the software, understanding the licensing issues and ensuring that we could safely leverage the code across our product line. We found that the selling company had fairly represented the integrity of their code. Black Duck allowed us to protect against any possible future issues with undocumented dependencies, and the assessment ultimately supported and helped justify the acquisition."